# Ambiente Lógico e Controle de Acesso

## 1) Relação entre Controle de Acesso Lógico, Autenticação e Autorização

O controle de acesso lógico é um conjunto de mecanismos que protege sistemas e dados contra acessos não autorizados, assegurando que apenas usuários devidamente identificados possam acessar recursos específicos. Ele depende fundamentalmente dos processos de autenticação e autorização.

Autenticação é o processo de verificar a identidade de um usuário (por exemplo, através de login e senha, autenticação biométrica ou token).
Autorização ocorre após a autenticação e determina quais ações o usuário está autorizado a realizar, de acordo com seu perfil e privilégios.

Esses três elementos funcionam juntos de forma sequencial: primeiro a identidade do usuário é confirmada (autenticação), depois o sistema verifica o que o usuário pode fazer (autorização), e por fim o controle de acesso lógico aplica essas regras para garantir que a segurança da informação seja mantida.

Exemplo prático: Em uma empresa onde trabalhei, o acesso ao sistema de folha de pagamento era restrito. Após o login com senha (autenticação), apenas os funcionários do RH conseguiam visualizar e editar dados salariais (autorização). Outros setores não tinham acesso a essas informações.

## 2) Importância da Política de Senhas Eficaz e Riscos de Senhas Fracas ou Compartilhadas

Uma política de senhas eficaz é fundamental para proteger sistemas e informações de acessos indevidos. Senhas fracas, previsíveis ou compartilhadas facilitam ataques como força bruta, engenharia social e acessos não autorizados.

Riscos de senhas fracas ou compartilhadas:
- Acesso de intrusos aos sistemas internos.
- Roubo de informações sensíveis (dados financeiros, propriedade intelectual).
- Comprometimento da integridade dos sistemas (modificações não autorizadas).
- Dificuldade em rastrear atividades suspeitas.

Boas práticas:
- Exigir senhas fortes (letras, números e símbolos).
- Trocar senhas periodicamente.
- Proibir senhas baseadas em informações pessoais.
- Nunca compartilhar senhas.

Exemplo prático: Vi casos em que equipes compartilhavam uma senha administrativa entre vários funcionários, o que resultou em perda de rastreabilidade em um incidente de acesso não autorizado.

### 3) Administração e Revisão Periódica de Privilégios de Usuários

A administração adequada dos privilégios de usuários é essencial para garantir que cada colaborador tenha acesso apenas aos recursos necessários para suas funções (princípio do mínimo privilégio). A revisão periódica desses privilégios ajuda a detectar e corrigir excessos ou acessos desnecessários.

Importância:
- Reduz a superfície de ataque.
- Impede manutenção de acessos antigos.
- Facilita auditorias e conformidade (ISO 27001).

Boas práticas:
- Perfis de acesso baseados em funções (RBAC).
- Revisões periódicas (ex.: semestrais).
- Gestão automatizada de acessos.

Exemplo prático: Em um projeto, a revisão semestral de acessos identificou usuários inativos com privilégios elevados, eliminando riscos.

### 4) Trabalho Remoto e Dispositivos Móveis: Desafios e Controles

O trabalho remoto e o uso de dispositivos móveis ampliam a exposição da organização a riscos de segurança.

Desafios:
- Dispositivos pessoais infectados.
- Interceptação de dados em redes públicas.
- Perda ou roubo de dispositivos.

Controles recomendados:
- VPNs para conexões seguras.
- Autenticação forte (2FA).
- Políticas de BYOD.
- Criptografia obrigatória.
- Gerenciamento remoto (MDM).

Exemplo prático: Durante a pandemia, VPNs foram exigidas para home office, proibindo uso de dispositivos pessoais não gerenciados.

### 5) Importância dos Registros de Logs (Trilhas de Auditoria)

Os registros de logs são essenciais para detectar incidentes de segurança, realizar auditorias e garantir a integridade dos sistemas.

Informações a registrar:
- Identificação do usuário.
- Tipo de evento.
- Data e hora.
- Sucesso ou falha.
- Origem do acesso.
- Dados ou sistemas afetados.

Utilização dos registros:
- Investigar incidentes.
- Provar conformidade.
- Identificar comportamentos anômalos.

Exemplo prático: Em uma auditoria ISO 27001, a falta de logs completos resultou em não conformidade grave.